REPRESENTATIONS OF DEFINITE BINARY QUADRATIC FORMS OVER $\mathbf{F}_q[t]$

JEAN BUREAU AND JORGE MORALES

Abstract. In this paper, we prove that a binary definite quadratic form over $\mathbf{F}_q[t]$, where q is odd, is completely determined up to equivalence by the polynomials it represents up to degree $3m-2$, where m is the degree of its discriminant. We also characterize, when $q > 13$, all the definite binary forms over $\mathbf{F}_q[t]$ that have class number one.

1. Introduction

It is a natural question to ask whether binary definite quadratic forms over the polynomial ring $\mathbf{F}_q[t]$ are determined, up to equivalence, by the set of polynomials they represent. Here $\mathbf{F}_q$ is the finite field of order q and q is odd.

The analogous question over $\mathbf{Z}$ has been answered affirmatively – with the notable exception of the forms $X^2 + 3Y^2$ and $X^2 + XY + Y^2$, which have the same representation set but are not equivalent – by Watson [13]. Several related results appear in the literature as far back as the mid-nineteenth century (see [14]).

We begin with the easier question whether the discriminant of a binary definite quadratic form over $\mathbf{F}_q[t]$ is determined by its representation set. In the classical case over $\mathbf{Z}$, Schering [11] showed that this is the case up to powers of 2. The same type of ideas are used here to show in the polynomial context that if Q and Q' represent the same polynomials up to degree $3m-2$, where $m = \max\{\deg \operatorname{disc}(Q), \deg \operatorname{disc}(Q')\}$, then $\operatorname{disc}(Q) = \operatorname{disc}(Q')$ (Proposition 3.5).

The main result of this paper is that if Q and Q' have the same discriminant and represent the same polynomials up to degree equal to their second successive minimum, then they are equivalent (Theorem 4.1). We show that if such forms were not equivalent, then there would be an elliptic curve over $\mathbf{F}_q$ that has more rational points than allowed by Hasse's bound. If the condition on the discriminants is omitted, then having the same representation set up to degree $3m-2$ is enough to conclude equivalence (Theorem 4.2).

The same questions can be asked for ternary definite quadratic forms. We show that in this case, the representation *sets* (as opposed to the representation *numbers*), are not enough in general to determine the equivalence class. We do so by constructing a family of counterexamples (Corollary 5.3). It turns out, however, that the representation *numbers*, that is the number of times that each polynomial is represented, are sufficient to determine the equivalence class of a ternary form, as it will be showed in an upcoming paper [2].

Finally, in Section 6, we show, assuming $q > 13$, that if a definite binary quadratic form Q has class number one (i.e. its genus contains only one equivalence class), then $\deg \operatorname{disc}(Q) \leq 2$ (Theorem 6.2).

2000 *Mathematics Subject Classification.* Primary: 11E25, 11E12. Secondary: 11E41, 11D09.

We are indebted to the referee for her/his useful remarks.

2. Notation and terminology

The following notation will be in force throughout the paper:

$\mathbf{F}_q$: The finite field of order q. We always assume q odd.
A : The polynomial ring $\mathbf{F}_q[t]$
K : The field of rational functions $\mathbf{F}_q(t)$
δ : A fixed non-square of $\mathbf{F}_q^\times$.

A quadratic form Q over A is a homogeneous polynomial

$$Q = \sum_{1\le i,j\le n} m_{ij} X_i X_j,$$

where $M = (m_{ij})$ is an $n\times n$ symmetric matrix with coefficients in A. The group $\mathbf{GL}_n(A)$ acts by linear change of variables on the set of such forms. Two forms in the same $\mathbf{GL}_n(A)$-orbit are called *equivalent*. Two forms in the same $\mathbf{SL}_n(A)$-orbit are called *properly equivalent*.

The *discriminant* of Q is defined by

$$\operatorname{disc}(Q) = (-1)^{n(n-1)/2}\det(M)$$

as an element of $A/\mathbf{F}_q^{\times 2}$. This is an invariant of the equivalence class of Q.

The *representation set* of Q is the set of polynomials

$$V(Q) = \{Q(\mathbf{x}) : \mathbf{x}\in A^n\},$$

and the *degree k representation set* is

$$V_k(Q) = \{Q(\mathbf{x}) : \mathbf{x}\in A^n,\ \deg Q(\mathbf{x})\le k\}.$$

The form Q is *definite* if it is anisotropic over the field $K_\infty = \mathbf{F}_q((1/t))$. This implies in particular that $n\le 4$.

A definite quadratic form Q is *reduced* if $\deg m_{ii}\le \deg m_{jj}$ for $i\le j$ and $\deg m_{ij} < \deg m_{ii}$ for $i<j$. Gerstein [5] showed that every definite quadratic form is equivalent to a reduced form and that two reduced forms in the same equivalence class differ at most by a transformation in $\mathbf{GL}_n(\mathbf{F}_q)$. In particular, the increasing sequence of degrees of the diagonal terms of a reduced form

$$(\deg m_{11}, \deg m_{22}, \dots, \deg m_{nn})$$

is an invariant of its equivalence class. This sequence is called the *successive minima* of Q and will be denoted by $(\mu_1(Q), \mu_2(Q), \dots, \mu_n(Q))$.

In the case of binary forms, which are the main topic of this paper, we will often write

$$Q = (a, b, c)$$

for the quadratic form

$$Q = aX^2 + 2bXY + cY^2.$$

For binary forms, it is easy to see that being definite means simply that $\operatorname{disc}(Q) = b^2 - ac$ has either odd degree or has even degree and non-square leading coefficient. Also, Q reduced translates into the condition

$$\deg b < \deg a \le \deg c. \tag{2.1}$$

If $Q = (a, b, c)$ is definite and reduced, then

$$\deg Q(x, y) = \max\{2\deg x + \mu_1, 2\deg y + \mu_2\} \tag{2.2}$$

for all $x, y \in A$, where μ_1 and μ_2 are the successive minima. When μ_1 and μ_2 have distinct parity, the equality (2.2) follows immediately from (2.1). When μ_1 and μ_2 have the same parity, (2.2) follows from (2.1) together with the fact that the leading coefficient of $-ac$ is a non-square by definiteness .

3. Successive minima and discriminant

Lemma 3.1. *Let $Q = (a, b, c)$ be a definite reduced form with successive minima $\mu_1 < \mu_2$. If $f \in A$ is represented by Q and $\mu_1 \leq \deg f < \mu_2$, then $f = r^2 a$ for some $r \in A$.*

Proof. Write $f = ar^2 + 2brs + cs^2$, with $r, s \in A$. If $\deg f < \mu_2$, then by (2.2) we must have $s = 0$, that is $f = r^2 a$. □

Lemma 3.2. *Let Q and Q' be definite binary forms over A with discriminants d and d' respectively. Let $m = \max\{\deg d, \deg d'\}$. If $V_m(Q) = V_m(Q')$, then $\mu_i(Q') = \mu_i(Q)$ $(i = 1, 2)$ and $\deg d = \deg d'$. Moreover, there are reduced bases in which the diagonal entries of the matrices of Q and Q' have the same leading coefficients.*

Proof. Let $Q = (a, b, c)$ and $Q' = (a', b', c')$ be in reduced form. Let $\mu_i = \mu_i(Q)$ and $\mu'_i = \mu'_i(Q)$ $(i = 1, 2)$. Since a is represented by Q', we clearly have $\mu'_1 \leq \mu_1$. If $\mu'_2 > \mu_2$, then

$$\mu'_1 \leq \mu_1 \leq \mu_2 < \mu'_2,$$

and applying Lemma 3.1 to Q', we get $a = a'r^2$ and $c = a's^2$ for some $s, r \in A$. In particular, $\mu_1 \equiv \mu_2 \pmod 2$. Let $k = (\mu_2 - \mu_1)/2$ and consider the expression

$$Q(t^k x, y) = t^{2k} a x^2 + 2t^k bxy + cy^2$$

with $x, y \in \mathbf{F}_q$. Using the inequality (2.1), we see that the coefficient of degree μ_2 of $Q(t^k x, y)$ is

$$a_{\mu_1} x^2 + c_{\mu_2} y^2, \tag{3.1}$$

where a_{μ_1} and c_{μ_2} are the leading coefficients of a and c respectively. Since $a_{\mu_1} c_{\mu_2} \neq 0$, the quadratic form (3.1) is non-degenerate over $\mathbf{F}_q$ and therefore represents all elements of $\mathbf{F}_q^\times$. If we choose in particular x, y so that (3.1) is not in the square class of $a'_{\mu'_1}$, then $Q(t^k x, y)$ cannot be represented by Q', since otherwise it would be of the form $r^2 a'$ by Lemma 3.1. Hence $\mu'_2 \leq \mu_2$, and by symmetry $\mu_1 = \mu'_1$ and $\mu_2 = \mu'_2$. The equality $\deg d = \deg d'$ follows immediately.

We can assume without loss of generality that $a = a'$. It remains to see that the leading coefficients of c and c' are in the same square class. When $\mu_1 \equiv \mu_2 \pmod 2$, the leading coefficients of c and of c' are both in the square class of $-\delta a_{\mu_1}$, where $\delta \in \mathbf{F}_q$ is a non-square. When $\mu_1 \not\equiv \mu_2 \pmod 2$, the leading coefficient of any element in $V(Q')$ whose degree has the same parity as μ_2 must be in the same square class as the leading coefficient of c'. This applies in particular to c.

□

Lemma 3.3. *Let Q be a primitive definite binary quadratic form over A with discriminant d and let p be an irreducible factor of d. Then Q represents a polynomial not divisible by p of degree $< \deg d$.*

Proof. Write Q in reduced form $Q = (a, b, c)$. Clearly either a or c satisfies the condition. □

Lemma 3.4. *Let Q be a primitive definite binary quadratic form over A with discriminant d. Let $p \in A$. Then each element of $V(Q)$ is congruent modulo p to an element in $V_{2\deg p + \deg d - 2}(Q)$.*

Proof. Let $\{e_1, e_2\}$ be a reduced basis for Q. Each element of $V(Q)$ is congruent modulo p to an element of the form $Q(x_1e_1 + x_2e_2)$ with $\deg x_i \leq \deg p - 1$. Clearly $\deg Q(x_1e_1 + x_2e_2) \leq 2(\deg p - 1) + \mu_2(Q) \leq 2(\deg p - 1) + \deg d$. □

Corollary 3.5. *Let Q and Q' be definite binary quadratic form over A with discriminants d, d' respectively. Let $m = \max\{\deg d, \deg d'\}$. If $V_{3m-2}(Q) = V_{3m-2}(Q')$ then $d' \in d\, \mathbf{F}_q^{\times 2}$.*

Proof. The statement is trivial if $m = 0$, so we shall assume through the proof that $m \geq 1$.

Notice that the equality of representation sets is preserved by scaling; hence Q and Q' may be assumed primitive.

We shall prove that for each irreducible polynomial $p \in A$:

$$V_{3m-2}(Q) \subset V_{3m-2}(Q') \quad \text{implies} \quad v_p(d') \leq v_p(d),$$

where $v_p(\cdot)$ denotes the p-adic valuation. This will show that $d = ud'$, where $u \in \mathbf{F}_q^\times$, and Lemma 3.2 shows that u must be a square.

Let $n = v_p(d)$ and $n' = v_p(d')$. If $\deg(p) > m$, then trivially $n = n' = 0$, so we may assume $\deg p \leq m$.

Let L be the A-lattice on which Q is defined and let $M = (p^n L^\sharp) \cap L$, where $L^\sharp$ is the dual lattice with respect to Q. Then it is easy to see that the form $Q_0 = p^{-n}Q|_M$ is integral and primitive and has discriminant d. By Lemma 3.3, Q_0 represents a polynomial u relatively prime to p with $\deg u \leq m - 1$. It follows that $p^n u$ is represented by Q and since $\deg p^n u \leq 2m - 1 \leq 3m - 2$ it must also be represented by Q'. In particular, $p^n u$ must be represented p-adically by Q'. Over A_p, the form Q' is equivalent to a diagonal form $(a, 0, p^{n'}b)$ where a, b are p-adic units. Then there exist $x, y \in A_p$ such that

$$p^n u = ax^2 + p^{n'}by^2. \tag{3.2}$$

It follows from (3.2) that if $n' > n$, then $n = v_p(ax^2) \equiv 0 \pmod 2$. Consider now the lattice $N = (p^{n/2}L^\sharp) \cap L$ and let $Q_1 = p^{-n}Q|_N$. One sees immediately that Q_1 is primitive, integral and $\mathrm{disc}(Q_1) = p^{-n}d$, so Q_1 is p-unimodular and thus $V(Q_1)$ contains representatives of all classes modulo p. In particular, Q_1 represents a polynomial w that is relatively prime to p and is in a different square class modulo p as a. Furthermore, by Lemma 3.4, w can be chosen so that $\deg w \leq 2\deg p + \deg(p^{-n}d) - 2$.

The polynomial $f = p^n w$ is obviously represented by Q and has degree $\leq 2\deg p + \deg d - 2 \leq 3m - 2$, so it is also represented by Q'. Writing f as in (3.2) and dividing by p^n we see that w is in the same square class as a, which is a contradiction. Hence $n' \leq n$.

□

4. Forms with the same representation sets in small degree

Theorem 4.1. *Assume $q > 3$. Let Q and Q' be two binary definite positive binary quadratic forms over A with the same discriminant and the same successive minima sequence (μ_1, μ_2). Suppose that $V_{\mu_2}(Q) = V_{\mu_2}(Q')$. Then Q and Q' are equivalent.*

Proof. Let $Q = (a, b, c)$ and $Q' = (a', b', c')$ be reduced forms. There is no loss of generality in making the following assumptions: $a = a'$ is monic and c, c' have same leading coefficients. When $\mu_1 \equiv \mu_2 \pmod 2$, the leading coefficients of c and c' can be assumed to be equal to $-\delta$, for the fixed non-square $\delta \in \mathbf{F}_q$.

1. Suppose that $\mu_1 \not\equiv \mu_2 \pmod 2$. Since c is also represented by Q, it is represented by Q'; hence, there are $f \in A$ and $\beta\ in \mathbf{F}_q$ such that $c = af^2 + 2b'f\beta + c'\beta^2$. The different parity of the successive minima implies that $\beta = \pm 1$. By changing b' into $-b'$ if necessary, we can assume that $\beta = 1$. Let $\varphi = \begin{pmatrix} 1 & f \\ 0 & 1 \end{pmatrix} \in \mathbf{GL}_2(\mathbf{F}_q)$. Then $Q'' := Q \circ \varphi = (a, b'', c')$, for some $b'' \in A$. Since $\det(\varphi) = 1$, it follows that $\operatorname{disc}(Q'') = \operatorname{disc}(Q) = \operatorname{disc}(Q')$; hence, $ac' - b''^2 = ac' - b'^2$. This leads to $b'' = \pm b'$.

2. Suppose that $\mu_1 \equiv \mu_2 \pmod 2$ and that $\mu_1 < \mu_2$. It follows from the equality of the discriminants that $\deg(c' - c) < \max\{\deg b, \deg b'\} < \deg a$.

If $b = b' = 0$, we conclude immediately that $c = c'$ by the equality of the discriminants. So we may assume $b \neq 0$.

Consider all the elements $au^2 + 2bu + c \in V(Q)$ with $u \in \mathbf{F}_q$. By assumption, the equation

$$au^2 + 2bu + c = ax^2 + 2b'xy + c'y^2 \tag{4.1}$$

is always solvable for some $x = x_k t^k + x_{k-1}t^{k-1} + \cdots + x_0 \in A$, where $k = (\mu_2 - \mu_1)/2$, and $y \in \mathbf{F}_q$.

Notice that for degree reasons, the polynomials a, b and c are linearly independent over $\mathbf{F}_q$ (recall that we are assuming $b \neq 0$), hence the left hand side of (4.1) takes exactly q values as u runs over $\mathbf{F}_q$. The equality of the leading coefficients in (4.1) gives

$$-\delta = x_k^2 - \delta y^2. \tag{4.2}$$

It is a standard fact that the number of pairs (x_k, y) satisfying (4.2) is $q + 1$ (see e.g. [6, Theorem 2.59]). Notice that if (x_k, y) is a solution of (4.2), then so is $(-x_k, y)$, thus the number of possible y's appearing in a solution of (4.2) is $(q - 1)/2 + 2 = (q + 3)/2$.

Since $q > (q + 3)/2$ by hypothesis, there must be two different values of u on the left-hand side of (4.1) with the same y on the right-hand side. In other words, there exist $u, v \in \mathbf{F}_q$, $u \neq v$, such that the system

$$\begin{cases} au^2 + 2bu + c = ax^2 + 2b'xy + c'y^2 \\ av^2 + 2bv + c = az^2 + 2b'zy + c'y^2 \end{cases} \tag{4.3}$$

has a solution (x, y, z), with $x, z \in A$ and $y \in \mathbf{F}_q$. By subtracting the two lines of (4.3), we get

$$a(u^2 - v^2) + 2b(u - v) = a(x^2 - z^2) + 2b'(x - z)y$$

By degree considerations $x^2 - z^2 = u^2 - v^2$ and hence x and z are constant. In particular $x_k = 0$ (since $k = (\mu_2 - \mu_1)/2 > 0$) and hence, by (4.2), we have $y^2 = 1$.

Going back to (4.1), we get

$$a(u^2 - x^2) + 2(bu - b'xy) = c' - c$$

As observed earlier, $\deg(c'-c) < \max\{\deg b, \deg b'\} < \deg a$. Thus the above equality implies $u^2 = x^2$. Thus $2(bu - b'xy) = 2u(b \pm b') = c' - c$. Replacing b' by $-b'$ if necessary, we can assume $2u(b+b') = c'-c$. Multiplying by $b-b'$ gives $2ua(c-c') = 2u(b^2 - b'^2) = (c'-c)(b-b')$ by the equality of the discriminants. Degree considerations again imply $c = c'$ and $b = \pm b'$.

3. Suppose that $\mu_1 = \mu_2 = n$. Write

$$\begin{aligned} a &= t^n + a_{n-1}t^{n-1} \cdots + a_0 \\ c &= -\delta t^n + c_{n-1}t^{n-1} + \cdots + c_0 \\ c' &= -\delta t^n + c'_{n-1}t^{n-1} + \cdots + c'_0 \\ b &= b_k t^k + \cdots + b_0 \\ b' &= b'_k t^k + \cdots + b'_0, \end{aligned}$$

where $k = \max\{\deg b, \deg b'\}$. If $b = b' = 0$, we are done, so we may assume $k \geq 0$ and $b'_k \neq 0$. Note that since $\operatorname{disc}(Q) = \operatorname{disc}(Q')$, we have $\deg(c - c') < k$ as in the previous case.

Since $V_n(Q) = V_n(Q')$, for any pair $(u,v) \in \mathbf{F}_q^2$, there exists a pair $(x,y) \in \mathbf{F}_q^2$ such that

$$Q(u,v) = Q'(x,y). \tag{4.4}$$

Taking the coefficients of t^n and t^k in the above polynomials, we get the system of quadrics:

$$\begin{cases} u^2 - \delta v^2 = x^2 - \delta y^2 \\ a_k u^2 + 2b_k uv + c_k v^2 = a_k x^2 + 2b'_k xy + c_k y^2, \end{cases} \tag{4.5}$$

which defines an algebraic curve E in $\mathbf{P}^3$. For every $(u,v) \in \mathbf{F}_q^2 \setminus \{0\}$, there is $(x,y) \in \mathbf{F}_q^2 \setminus \{0\}$ satisfying (4.5). Notice also that if a quadruplet (u,v,x,y) satisfies (4.5), so does $(u,v,-x,-y)$ and that the two sides of the first equation are forms anisotropic over $\mathbf{F}_q$, so $|E(\mathbf{F}_q)| \geq 2(q+1)$.

If the curve E given by (4.5) were smooth, then it would be an elliptic curve and by the Hasse estimate [12, Ch. V] we would have $|E(\mathbf{F}_q)| \leq 2\sqrt{q} + q + 1$, which would contradict the above count. Thus E cannot be a smooth curve.

It is also known that the intersection of two quadric hypersurfaces, say $Q_1 = 0, Q_2 = 0$, in $\mathbf{P}^m$ is a smooth variety of codimension 2 if and only if the binary form $\det(XQ_1 + YQ_2)$ of degree $m+1$ has no multiple factor (see e.g. [4, Remark 1.13.1] or [7, Chap. XIII §11]). In the case of our system (4.5), by computing explicitly the discriminant of $\det(XQ_1 + YQ_2)$, where Q_1, Q_2 are the two quaternary quadratic forms of (4.5), we get the condition

$$\delta^4 (b_k - b'_k)^4 (b_k + b'_k)^4 \left((a_k\delta + c_k)^2 - 4\delta b'^2_k\right)\left((a_k\delta + c_k)^2 - 4\delta b_k^2\right) = 0. \tag{4.6}$$

Since δ is not a square in $\mathbf{F}_q$ and $b'_k \neq 0$ by assumption, we must have either $b_k = \pm b'_k$ or $b_k = 0$ and $a_k\delta + c_k = 0$. We shall rule out the second possibility.

Since $V_n(Q) = V_n(Q')$, these sets span the same $\mathbf{F}_q$ -subspace of A; in particular b' must be an $\mathbf{F}_q$ -linear combination of a, b and c. Write

$$b' = \alpha a + \beta b + \gamma c,$$

with $\alpha, \beta, \gamma \in \mathbf{F}_q$. Taking terms of degree n gives

$$0 = \alpha - \delta\gamma,$$

which implies

$$b' = \gamma(\delta a + c) + \beta b.$$

Taking now terms of degree k we get

$$b'_k = \gamma(\delta a_k + c_k) + \beta b_k.$$

If $b_k = 0$ and $a_k\delta + c_k = 0$, then $b'_k = 0$, which is a contradiction with our assumption.

Thus $b_k = \pm b'_k$ is the only possibility. Replacing b by $-b$ if needed, we shall assume $b_k = b'_k$.

We shall now show that $b = b'$. Suppose by contradiction that $b \neq b'$ and let $m = \deg(b - b') < k$. Then, by the equality of the discriminants, $\deg(b^2 - b'^2) = m + k = n + \deg(c - c')$, which implies $\deg(c - c') < m$ and in particular $c_m = c'_m$.

Exactly the same argument that showed $b_k^2 = {b'}_k^2$ (just replace k by m in (4.5)) shows that $b_m^2 = b'^2_m$. Now consider the system

$$\begin{cases} a_m u^2 + 2b_m uv + c_m v^2 = a_m x^2 + 2b'_m xy + c_m y^2 \\ a_k u^2 + 2b_k uv + c_k v^2 = a_k x^2 + 2b'_k xy + c_k y^2. \end{cases} \tag{4.7}$$

Adding the two equations and combining the result with the first equation in (4.5) we get the system

$$\begin{cases} u^2 - \delta v^2 = x^2 - \delta y^2 \\ (a_k + a_m)u^2 + 2(b_k + b_m)uv + (c_k + c_m)v^2 = \\ \qquad (a_k + a_m)x^2 + 2(b'_k + b'_m)xy + (c_k + c_m)y^2, \end{cases} \tag{4.8}$$

Applying one more time the rational-point counting argument, this time to the above system, we conclude that $(b_m - b_k)^2 = (b'_m - b'_k)^2$, which yields $b_m b_k = b'_m b'_k$. Since $b_k = b'_k \neq 0$ we conclude $b_m = b'_m$, which contradicts the hypothesis that $m = \deg(b - b')$. Hence $b = b'$ as claimed. □

Finally, putting together Proposition 3.5, Lemma 3.2 and Theorem 4.1, we get our main result:

Theorem 4.2. *Assume $q > 3$. Let Q and Q' be definite binary quadratic forms over A with discriminants d and d' respectively. Let $m = \max\{\deg d, \deg d'\}$. If $V_{3m-2}(Q) = V_{3m-2}(Q')$, then Q and Q' are equivalent.*

5. The Ternary Case

In this section we give an example showing that in the case of ternary definite forms over A, the representation *sets* in general do not determine the discriminant, much less the equivalence class of the form [1].

Lemma 5.1. *Let $Q_a = X^2 + tY^2 - \delta(t + a^2)Z^2$, where $a \in \mathbf{F}_q^\times$. Then a polynomial $f \in A$ is represented by Q_a over A if and only if it is represented by Q_a over $A_{(t)} = \mathbf{F}_q[[t]]$.*

---

[1] However, the representation *numbers* do determine the equivalence class of such forms as showed in [1], [2].

Proof. By [3, Theorem 3.5], the form Q_a has class number one, so a polynomial $f \in A$ is represented by Q_a over A if and only if it is represented locally everywhere. At primes $\mathfrak{p}$ not dividing $\mathrm{disc}(Q_a) = \delta t(t + a^2)$, Q_a is unimodular and isotropic, hence represents everything. At $\mathfrak{p} = (t + a^2)$, since $t \equiv -a^2 \pmod{\mathfrak{p}}$, Q_a is equivalent to $X^2 - Y^2 - \delta(t + a^2)Z^2$ which also represents everything since $X^2 - Y^2$ already does so. Thus the only condition is at the prime $\mathfrak{p} = (t)$ (the condition at ∞ is automatic by reciprocity). □

Corollary 5.2. *For each $a \in \mathbf{F}_q^\times$, let Q_a be as in Lemma 5.1. The representation set $V(Q_a)$ does not depend upon the choice of a.*

Proof. By virtue of Lemma 5.1, it is enough to notice that Q_a is equivalent to $X^2 + tY^2 - \delta Z^2$ over $\mathbf{F}_q[[t]]$, which is independent of a. □

Corollary 5.3. *Assume $q \geq 5$ and choose $a, b \in \mathbf{F}_q^\times$ such that $a^2 \neq b^2$. Then $V(Q_a) = V(Q_b)$ but $\mathrm{disc}(Q_a) \neq \mathrm{disc}(Q_b)$.*

Proof. Clear by Corollary 5.2. □

6. Primitive binary forms of class number one

In this section, we characterize primitive binary quadratic forms over $A = \mathbf{F}_q[t]$ of class number one. Although it should be possible, in principle, to deduce the results below from general formulas such as the ones in [9], we prefer to give here a direct argument.

We begin by a statement on orders in quadratic extensions of $K = \mathbf{F}_q(t)$.

Corollary 6.1. *Let $D = f^2 D_0 \in A$, where D_0 is a square-free polynomial of either odd degree or of even degree and non-square leading coefficient, and $f \in A$ is a monic polynomial. Let $B = A[\sqrt{D}]$. Assume that $\mathrm{Pic}\,(B)$ is an abelian 2-group and has at most one cyclic component of order 4 and all other components of order 2. Then*

1. *If $\deg D_0 > 0$ and $q > 13$, then D is square-free (i.e. $f = 1$) and $\deg D \leq 2$.*
2. *If $\deg D_0 = 0$ and $q > 5$, then $\deg D \leq 2$.*

Proof. Let $\mathfrak{O} = A[\sqrt{D_0}]$. Notice that $\mathfrak{O}$ is the maximal A-order in the field $E = K(\sqrt{D_0})$ and that f is the conductor of B in $\mathfrak{O}$.

There is an exact sequence

$$1 \longrightarrow \frac{\mathfrak{O}^\times}{B^\times} \longrightarrow \frac{(\mathfrak{O}/f\mathfrak{O})^\times}{(A/fA)^\times} \longrightarrow \mathrm{Pic}\,(B) \longrightarrow \mathrm{Pic}\,(\mathfrak{O}) \longrightarrow 1. \tag{6.1}$$

1. Assume $\deg D_0 > 0$. Then $\mathfrak{O}^\times = B^\times = \mathbf{F}_q^\times$ and we get a shorter exact sequence

$$1 \longrightarrow \frac{(\mathfrak{O}/f\mathfrak{O})^\times}{(A/fA)^\times} \longrightarrow \mathrm{Pic}\,(B) \longrightarrow \mathrm{Pic}\,(\mathfrak{O}) \longrightarrow 1. \tag{6.2}$$

Let h be the radical of f (i.e. the product of all irreducible monic divisors of f). The subgroup $(1 + h\mathfrak{O}/f\mathfrak{O})/(1 + hA/fA)$ of $(\mathfrak{O}/f\mathfrak{O})^\times/(A/fA)^\times$ has order $q^{\deg f - \deg h}$ and is a 2-group by the exact sequence (6.2), so we must have $f = h$, i.e. f is square-free.

Let π be an irreducible factor of f of degree d. Then $(\mathfrak{O}/\pi\mathfrak{O})^\times/(A/\pi A)^\times$ is a direct factor of $(\mathfrak{O}/f\mathfrak{O})^\times/(A/fA)^\times$ and is cyclic of order q^d-1 or q^d+1 (according to whether π is split or inert in E) or is isomorphic to the additive group $\mathbf{F}_{q^d}$ when π is ramified. Clearly the latter case is impossible since q is odd and in the first two cases we must have $q^d \pm 1 = 2$ or 4, which is also impossible when $q > 5$. Hence $f = 1$, D is square-free and $B = \mathfrak{O}$.

Let r be the number of irreducible factors of D. It is well-known that the 2-rank of $\mathrm{Pic}\,(\mathfrak{O})$ is $r-1$. Hence, under our present hypotheses, $|\mathrm{Pic}\,(\mathfrak{O})| \le 2^r$. The order of $\mathrm{Pic}\,(\mathfrak{O})$ is essentially the class number h_E of E; more precisely $|\mathrm{Pic}\,(\mathfrak{O})| = h_E$ if $\deg D$ is odd and $|\mathrm{Pic}\,(\mathfrak{O})| = 2h_E$ if $\deg D$ is even [10, Proposition 14.7].

Using the lower bound for h_E given by the Riemann Hypothesis [10, Proposition 5.11], we get

$$\begin{array}{lclll} (\sqrt{q}-1)^{\deg D-1} & \le & 2^r & \text{if} \quad \deg D & \text{is odd;} \\ (\sqrt{q}-1)^{\deg D-2} & \le & 2^{r-1} & \text{if} \quad \deg D & \text{is even.} \end{array}$$

When $\deg D \ge 3$, using the above inequalities and the obvious fact that $r \le \deg D$, we get easily the inequality $\log_2(\sqrt{q}-1) \le 3/2$, which is impossible if $q > 13$.

2. Assume $\deg D_0 = 0$ and $\deg f > 0$. Then $\mathfrak{O} = \mathbf{F}_{q^2}[t]$, so $\mathrm{Pic}\,(\mathfrak{O}) = \{1\}$, $\mathfrak{O}^\times = \mathbf{F}_{q^2}^\times$ and $B^\times = \mathbf{F}_q^\times$. The exact sequence (6.1) becomes

$$1 \longrightarrow \frac{\mathbf{F}_{q^2}^\times}{\mathbf{F}_q^\times} \longrightarrow \frac{(\mathfrak{O}/f\mathfrak{O})^\times}{(A/fA)^\times} \longrightarrow \mathrm{Pic}\,(B) \longrightarrow 1 \tag{6.3}$$

Let p be the characteristic of $\mathbf{F}_q$. Taking p-parts in the sequence above (i.e. tensoring by $\mathbf{Z}_p$), we get $[(\mathfrak{O}/f\mathfrak{O})^\times/((A/fA)^\times)]_p = 0$. Exactly the same argument as in Case 1 shows that f must be square-free. Hence

$$\frac{(\mathfrak{O}/f\mathfrak{O})^\times}{(A/fA)^\times} = \prod_{\pi|f} \frac{(\mathfrak{O}/\pi\mathfrak{O})^\times}{(A/\pi A)^\times}, \tag{6.4}$$

where π runs over all irreducible monic divisors of f.

Notice that the factors on the right-hand side of (6.4) are cyclic of order $q^{\deg\pi}+1$ if $\deg\pi$ is odd, and $q^{\deg\pi}-1$ if $\deg\pi$ is even.

Let π be an irreducible factor of f of even degree, say $\deg\pi = 2m$, then, by the exact sequence (6.3), $(q^{2m}-1)/(q+1)$ must be a 2-power ≤ 4. This is possible only when $m = 1$ and $q = 3$ or $q = 5$. Similarly, if $\deg\pi$ is odd, say $\deg\pi = 2m+1$, then $(q^{2m+1}+1)/(q+1)$ must be a 2-power, but it is always an odd number, so the only possibility is $m = 0$, i.e. $\deg\pi = 1$. Thus, when $q > 5$, f is a product of linear factors.

If $q+1$ is divisible by an odd prime ℓ, then, since $\mathrm{Pic}\,(B)$ is a 2-group, taking ℓ-parts in (6.3) shows that there must be only one factor in the decomposition (6.4), i.e. f is irreducible (necessarily linear as shown above).

The only case left is when $q+1$ is a 2-power. Notice that the factors on the right-hand side of (6.4) are all cyclic of order $q+1$, since all the π's are linear. By the hypothesis on $\mathrm{Pic}\,(B)$, if there is more than one factor in (6.4), then $q+1$ is a 2-power ≤ 4. This is impossible if $q > 3$. Thus, also in this case, f has only one irreducible, necessarily linear, factor. $\square$

Let (V,Q) be a quadratic space over the field $K=\mathbf{F}_q(t)$. Let $L\subset V$ be an A-lattice and let $\mathrm{Gen}(L)$ be the set of lattices of V in the genus of L. The orthogonal group $\emptyset(V,Q)$ acts on $\mathrm{Gen}(L,Q)$ and the number of orbits (which is well-known to be finite) is called the *class number* of L and will be denoted by $h(L,Q)$, or simply $h(Q)$ when the underlying lattice is obvious. The number of orbits of the action of the subgroup $\mathbf{SO}(V,Q)$ on $\mathrm{Gen}(L,Q)$ will be denoted by $h^+(L,Q)$. Since $\mathbf{SO}(V,Q)$ has index 2 in $\emptyset(V,Q)$, we have $h^+(L,Q)\le 2h(L,Q)$.

If (L,Q) is primitive of rank 2, then $h^+(L,Q)$ depends only on $D=\mathrm{disc}(L,Q)$. Indeed, let G_D be the set of classes of primitive binary quadratic forms of discriminant D up to orientation-preserving (i.e. of determinant 1) linear transformation. This set is a group for Gaussian composition [8] and there is a natural exact sequence relating G_D and $\mathrm{Pic}\,(B)$, where $B=A[\sqrt{D}]$, (see [8, §6]), which in our situation is

$$1\longrightarrow \mathbf{F}_q^\times/\mathbf{F}_q^{\times 2}\longrightarrow G_D\longrightarrow \mathrm{Pic}\,(B)\to 1. \tag{6.5}$$

The *principal genus* consists of forms in the genus of the norm form X^2-DY^2 of B, and their classes in G_D form a subgroup G_D^0. The different genera are cosets for this subgroup and hence they have all the same number of classes, i.e. $h^+(L,Q)=|G_D^0|$ for all primitive quadratic lattices (L,Q) of discriminant D. It is also well-known (and easy to see) that G_D/G_D^0 is 2-elementary.

Theorem 6.2. *Let Q be a definite primitive binary quadratic form over A, where $q>13$. If $h(Q)=1$ then $\deg\mathrm{disc}(Q)\le 2$.*

Proof. If $h(Q)=1$, then $h^+(Q)=|G_D^0|\le 2$ and by the remarks above G_D is an abelian 2-group with at most one cyclic component of order 4 and all others of order 2. So is $\mathrm{Pic}\,(B)$ by the exact sequence (6.5) and we conclude by Proposition 6.1. □

Remark. Theorem 6.2 is incorrect without the assumption $q>13$. Here is a counterexample for $q=13$.

Let $D=t(t^2-1)$ and let E be the elliptic curve over $\mathbf{F}_{13}$ given by the equation $s^2=D$. Let $B=A[\sqrt{D}]$. Then $\mathrm{Pic}\,(B)=E(\mathbf{F}_{13})\cong\mathbf{Z}/2\mathbf{Z}\oplus\mathbf{Z}/4\mathbf{Z}$. It is easy to see that the exact sequence (6.5) is split in this case, so $G_D^0=2G_D=2E(\mathbf{F}_{13})\cong\mathbf{Z}/2\mathbf{Z}$. Let Q_0 be a form whose class $[Q_0]$ generates G_D^0. Then the genus of any form Q of discriminant D consists of the classes $[Q]$ and $[Q']=[Q]+[Q_0]$ in G_D. If $[Q]$ has order 4, then $[Q']=-[Q]$ i.e. Q and Q' are (improperly) equivalent and thus $h(Q)=1$. An explicit example is $Q=(t-5,4,-(t^2+5t+11))$, which corresponds to the point $P=(5,4)$ of order 4 in $E(\mathbf{F}_{13})$.

Theorem 6.2 gives a converse of a result of Chan-Daniels [3]. We summarize this in the following statement:

Corollary 6.3. *Assume $q>13$. A binary definite quadratic form Q over A of discriminant D has class number one if and only if it satisfies one of the following conditions:*

1. $\deg D\le 1$.
2. $\deg D=2$ *and* $\mu_1(Q)=1$.
3. $\deg D=2$, $\mu_1(Q)=0$ *and* D *is reducible.*

Proof. The "if" part follows from [3, Lemma 3.7] and the ensuing remark. The "only if" part is a consequence of Theorem 6.2. □

References

1. Jean Bureau, *Representation properties of definite lattices in function fields*, Ph.D. thesis, Louisiana State University, 2006.
2. Jean Bureau and Jorge Morales, *Isospectral definite ternary* $\mathbf{F}[t]$*-lattices*. Preprint 2008. To appear J. Number Theory.
3. Wai Kiu Chan and Joshua Daniels, *Definite regular quadratic forms over* $\mathbb{F}_q[T]$, Proc. Amer. Math. Soc. **133** (2005), no. 11, 3121–3131 (electronic).
4. Jean-Louis Colliot-Thélène, Jean-Jacques Sansuc, and Peter Swinnerton-Dyer, *Intersections of two quadrics and Châtelet surfaces. I*, J. Reine Angew. Math. **373** (1987), 37–107.
5. Larry J. Gerstein, *Definite quadratic forms over* $\mathbb{F}_q[x]$, J. Algebra **268** (2003), no. 1, 252–263.
6. ———, *Basic quadratic forms*, Graduate Studies in Mathematics, vol. 90, American Mathematical Society, 2008.
7. W. V. D. Hodge and D. Pedoe, *Methods of algebraic geometry. Vol. II. Book III: General theory of algebraic varieties in projective space. Book IV: Quadrics and Grassmann varieties*, Cambridge, at the University Press, 1952.
8. Martin Kneser, *Composition of binary quadratic forms*, J. Number Theory **15** (1982), no. 3, 406–413.
9. Ulrike Korte, *Class numbers of definite binary quadratic lattices over algebraic function fields*, J. Number Theory **19** (1984), no. 1, 33–39.
10. Michael Rosen, *Number theory in function fields*, Graduate Texts in Mathematics, vol. 210, Springer-Verlag, New York, 2002.
11. M. Schering, *Théorèmes relatifs aux formes quadratiques qui représentent les mêmes nombres*, J. Math. Pures Appl. **2** (1859), no. IV, 2ème série, 253–269.
12. Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986.
13. G. L. Watson, *Determination of a binary quadratic form by its values at integer points*, Mathematika **26** (1979), no. 1, 72–75.
14. ———, *Acknowledgement: "Determination of a binary quadratic form by its values at integer points" [Mathematika* **26** *(1979), no. 1, 72–75; MR 81e:10019]*, Mathematika **27** (1980), no. 2, 188 (1981).

Mathematics Department, Louisiana State University, Baton Rouge, LA 70803-4918, U.S.A.
E-mail address: jbureau@math.lsu.edu

Mathematics Department, Louisiana State University, Baton Rouge, LA 70803-4918, U.S.A.
E-mail address: morales@math.lsu.edu